Fairfax County Internal Audit Office

Department of Public Works and Environmental Services
Department of Information Technology
Fairfax Inspections Database Online (FIDO) Application Audit
Final Report

April 2010

"promoting efficient & effective local government"

Executive Summary

In March 2006, the Department of Public Works and Environmental Services (DPWES) and the Department of Planning and Zoning (DPZ) replaced the county's legacy Inspection Services Information System (ISIS) with the Commercial-of-the-Shelf (COTS) application, the Fairfax Inspections Database Online (FIDO). The FIDO application provides a single software solution that meets the needs of the multiple agencies involved in permits, inspections, licenses, fee collection, and complaints management processes. Currently the FIDO application is used by DPWES, DPZ, Fire and Rescue Department, Health Department, and the Strike Team.

This audit is a first phase examination of the FIDO system, which begin with DPWES. Our audit found that there were controls over data input to ensure permit application data were inputted into the FIDO application completely and timely. The FIDO application had built-in edit checks to ensure the initial recording of data into the FIDO application was accurate. The FIDO application data and system files were backed up on a daily basis. We also determined that permit application filing fees and permit fees were calculated correctly and collected before a permit was issued. Reconciliation was performed to ensure payments are recorded correctly into the FIDO application. However, compliance with the county's Information Technology Security Policy 70-05.01 related to account management, password, administrative access, and data recovery, needs to be strengthened. The primary issues noted were:

<u>DPWES</u>

- The outstanding issues listed on the Daily Exception Logout Report and the Finalled Permits with Outstanding Issues Report for the period of January 2009 to June 2009 were not resolved in a timely manner.
- DPWES did not establish procedures to periodically review the user list and determine whether it remained appropriate. The user list for the FIDO application was not up-to-date.
- No formal access request form was in place for changing and removing users in the FIDO application.
- Procedures were not established for documenting administrative final approval permit applications.
- Ten out of 112 sampled permit application paper files could not be located.
- The cashier who performed the payments reconciliation did not sign and date on the reconciliation document.

<u>DIT</u>

- The FIDO application and the Oracle database did not generate an audit trail for the administrative user ID IMSV7 activities, which has the ability to modify the system processing capabilities.
- The FIDO system administrator had the privileges to view all users' passwords.
- The FIDO application did not enforce the use of strong passwords.
- The current version of FIDO application Oracle database could not be recovered at the county hot site.

Scope and Objectives

This audit was performed as part of our fiscal year 2009 Annual Audit Plan and was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. This audit covered the period of January through June 2009, and our audit objectives were to determine that:

- All the forms of application information are inputted into the FIDO application completely and timely and updated accordingly.
- Fee payments are calculated correctly and collected timely.
- Access controls and management trails are established to ensure data is adequately protected from unauthorized amendment, loss or leakage.
- The application is in compliance with the county's IT Security Policy.
- Backup and recovery is tested and documented.

Methodology

Our audit approach included a review and analysis of internal controls over the FIDO application data input and permit application processing. We interviewed appropriate employees to understand the permit application process, observed employees' work functions, determined if controls were in place to prevent data from unauthorized modification, and tested permit application transactions on a sample basis.

Our audit did not examine all general controls, such as system software, segregation of duties and security program planning and management, over the FIDO application. Our transaction testing did rely on those controls; therefore, this was a scope limitation. The potential impact of this circumstance on our findings was that some portion of transaction data may be erroneous.

Findings, Recommendations, and Management Response

Department of Public Works and Environmental Services

1. Exception Reports

The existing management reports could be generated on a monthly or daily basis. Currently only daily exception reports were available to the managers. The manager assigned staff to investigate the permits listed on the Daily Exception Logout Report and Finalled Permits with Outstanding Issues report and resolve the outstanding issues. The exception reports were generated on a daily basis; however, they only listed permits with outstanding issues that occurred on the date the report was generated. Whether the outstanding issues were resolved or not for a permit, the following day's exception report did not list these permits. IAO requested the IT support staff to run

these two exception reports for the time frame between January 1, 2009, and June 30, 2009, and found 26 permits with outstanding issues.

DPWES ran two exception reports from the Crystal Report system on a daily basis, which were the Daily Exception Logout Report and the Finalled Permits with Outstanding Issues Report. The Daily Exception Logout Report listed the permits issued with outstanding fees, reviews and other conditions. The Finalled Permits with Outstanding Issues Report listed the permits that had passed the final inspection but with outstanding issues. These two reports were forwarded to the permit and inspection group via e-mail.

A third report, the Permits Scheduled for Final Inspection With Outstanding Issues report, which listed the permits that were scheduled for final inspection but had outstanding issues, was generated on a daily basis and distributed to the inspection supervisor. The inspection supervisor could inform the inspector to stop running the final inspection unless the outstanding issues were resolved. If the final inspection was passed and updated into the FIDO application while outstanding issues were not resolved, the permit was listed on the Finalled Permits with Outstanding Issues report.

For the permits that passed the final inspection with unpaid fees, the county may lose revenue unless permits listed on the exception reports are investigated and the outstanding issues are resolved in a timely manner.

Recommendation: We recommend DPWES run accumulated monthly exception reports for the Daily Exception Logout Report and Finalled Permits with Outstanding Issues Report in addition to the daily exception report. The manager should review both exception reports to ensure that all outstanding issues are resolved timely.

Management Response: Exception reports are generated and emailed to appropriate staff on a daily basis to ensure that outstanding issues are resolved in a timely manner. Additionally, exception reports with accumulated data have been available on demand for managers since the reports were introduced in 2008. In response to the recommendation of the auditor, accumulated exception reports are now automatically emailed to managers and other appropriate staff on a biweekly basis to ensure that all issues identified on the daily reports have been resolved.

2. User Access Maintenance

The user list for the FIDO application was not up-to-date. We used ACL to randomly select a sample of 30 users from the list and noted that nine users should be removed from the FIDO application because these users either transferred to other departments or left the county and no longer have a business reason for system access. For the users who left the county, their county network's access rights were removed, which served as a compensating control.

Fairfax County Information Technology Security Policy 70-05.01 states that system administrators or other designated staff:

- Are responsible for removing the accounts of individuals who change roles within Fairfax County or are separated from their relationship with Fairfax County.
- Shall have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.
- Shall have a documented process for periodically reviewing existing accounts for validity.

It is very important to notify the system administrator immediately when an employee is terminated or, for some other reason, is no longer authorized access to the FIDO application. Terminated employees who continue to have access to critical or sensitive resources pose a threat, especially those individuals who may have left under acrimonious circumstances. DPWES did not establish procedures to periodically review the user list and determine whether it remained appropriate.

Recommendation: We recommend that DPWES establish and implement procedures to periodically review the FIDO application user list and assign responsibility for notifying the system administrator when an employee is terminated or, for some other reason, is no longer authorized access to the FIDO application.

Management Response: Supervisors throughout the agency have been assigned responsibility for notifying IT Services when an employee is terminated or, for some other reason, is no longer authorized access to the FIDO application (standardized form created and implemented on December 7, 2009).

DPWES does not currently have direct access to the FIDO application user list referenced in this recommendation. DPWES concurs with the recommendation and is working with DIT to establish a solution that will enable LDS to view and manage user access to FIDO. In the meantime, DIT has agreed to regularly provide necessary reports for periodic review, validation, and update. The anticipated completion date is March 31, 2010.

3. Documentation for System Access

DPWES utilized the DPWES Mainframe and Network Access Request form to document the requests for adding new users to the FIDO application. Other requests for changing and removing the FIDO application users were made through e-mails or phone conversations. There was no formal access request form to document the change authorization. In addition, the DPWES IT staff did not keep all the e-mail communications for the requests of changing access rights to the FIDO application.

Fairfax County Information Technology Security Policy 70-05.01 states: All accounts created shall have an associated request and approval that is appropriate for the Fairfax County system or service. System Administrators or other designated staff:

- Are responsible for removing the accounts of individuals who change roles within Fairfax County or are separated from their relationship with Fairfax County.
- Shall have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.

- Shall have a documented process for periodically reviewing existing accounts for validity.

The lack of a standardized access request form for changing and updating users' access rights creates risks of granting users excessive access rights to perform their duties, changing users' access rights without manager's approval, and keeping transferred or terminated users active in the system.

Recommendation: We recommend that DPWES establish a standard access request form to document authorization and modification of access privileges approved by an authorized manager and maintain the completed forms on file. Changes to user's access rights should be authorized and documented.

Management Response: DPWES has developed and implemented new FIDO access procedures and a standard FIDO access request form for new FIDO accounts, existing account modification, and removal from the system.

The access request form was developed for use by other FIDO agencies and has been reviewed and approved by the multi-agency FIDO Core Team. The new FIDO access form has been provided to the other user agencies and will be implemented by each agency as they see fit.

4. Documentation for Administrative Final Permits Applications

The commercial inspection group performed an administrative final approval for permits that were more than three or four years old. After a permit was issued, it was the permit's holder's responsibility to call the inspection division to schedule all the required inspections. But sometimes because of various reasons, the permit holder did not call for inspection after a permit was issued. An old open permit was brought to the inspection division's attention when a "due diligence request for open building code violations" was received through the Freedom of Information Act (FOIA). The inspection group supervisors investigated the permits and made the administrative final decision based on permit type and their professional judgments. There were no written procedures for implementing administrative final approvals. All the administrative finals were marked as "final inspection" in the FIDO application. In the "comments" field, the supervisor normally wrote"admin. final by supervisor's name." The supervisor did not document the criteria used to support the "admin. final" decision.

Established policies and procedures are a means to achieve proper controls over a business process. Management should clearly define who is authorized to perform the administrative final decision, and under what circumstance an administrative final decision can be made.

There were no written procedures for implementing an administrative final. The county cannot support the reasons why an administrative final decision is made based on what is recorded in the FIDO application.

Recommendation: We recommend that DPWES Land Development Services develop and implement a list of criteria to document how an administrative final decision is reached.

Management Response: LDS has developed and implemented criteria to document how decisions are made in regard to providing "administrative final inspections" on older permit records.

5. Missing Documentation

The Inspection Requests & Records Section of the DPWES/LDS was responsible for the maintenance of the paper files related to permits. The files were stored in a dedicated room within the branch together with a log for signing in/out the documents. No staff was assigned to monitor the removal of files, or to verify that the log was completed. Branch personnel assisted with the retrieval of files when necessary. The applications paperwork from ten permits out of a sample of 112 could not be located.

The supporting documentation paper files should be available when needed. If removed from the file room, sufficient information must be entered in the paper log so that the files can be located if necessary. The misplacement or loss of paper files can negatively impact dispute resolution, customer service, and various other functions of DPWES due to the lack of complete evidence of actions taken by all parties.

The staff of the Inspection Scheduling Branch of the DPWES/LDS was also responsible for scheduling inspections and answering calls about inspections. There was no one assigned to ensure that the file room log was completed when files were removed. The room was not locked during business hours.

Recommendation: We recommend that DPWES develop and implement written procedures that require the use of the log for signing in/out files. We also recommend that the inspections scheduling staff control access to the file room such that the completion of the log prior to signing in/out the files can be verified.

Management Response: Written procedures for handling records for building and trade permits, plans, and inspection records in the custody of Inspection Records and Requests (IR&R) were developed and implemented. The procedures include controlling access to the records and policies for signing in and out documents.

6. Financial Reconciliation

Cashiers performed the reconciliation on a daily basis to ensure payments were recorded correctly into the FIDO application. However, the cashier who performed the reconciliation did not sign and date the reconciliation document to evidence proper actions. This documentation provides a record of oversight activity and the persons responsible. Although the Financial Management Group maintains all documentation supporting the reconciliation, there was no record to prove who performed the reconciliation and when the reconciliation was being performed.

Recommendation: We recommend DPWES Land Development Services Financial Management Group require that the staff performing the reconciliation sign and date the work performed.

This recommendation was implemented during the audit. No management response is required.

Management Response: Implemented during the audit.

Department of Information Technology

7. Userid IMSV7

The FIDO system configuration (i.e. programming) tool set and IMSV7 administrative user ID support all FIDO maintenance and customization activities. The DIT Land Planning Service (LPD) IT support group used administrative user ID IMSV7 to:

- Design, develop and maintain FIDO applications (permits, licenses, code violations).
- Develop Oracle database stored procedures and trigger.
- Create, and maintain user ID profiles.
- Refine and enhance work flow processes (fee collection, data validation, safety reviews).
- Create and modify the FIDO presentation layer (i.e. data entry and inquiry screens).

The IMSV7 password is the gateway to all the FIDO operational performance, maintenance and enhancement activities. Due to the system configuration, the IMSV7 database password has never been changed. The IMSV7 application password was rarely changed. The most recent IMSV7 application password change was in the summer of 2007. There were ten LPD IT staff with access to IMSV7 passwords. The LPD used an internally designed change management spreadsheet to log the IMSV7 activities. However, not all IMSV7 activities were logged and monitored. The FIDO application or the Oracle database did not generate an audit trail for the IMSV7 activities.

Audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem analysis. An audit trail should include sufficient information to establish what events occurred and who (or what) caused them. In general, an audit trail should specify when the event occurred, the user ID associated with the event, the program or command used to initiate the event, and the result.

The LPD IT support group has update access to the FIDO application production environment. The IMSV7 database user ID also has the database administrator (DBA) access rights. Without a sufficient audit trail and timely, independent review, unauthorized or erroneous actions could be introduced, affecting the county's financial transactions, or confidential county citizen complaint information.

Recommendation: We recommend that an audit trail be generated every time the IMSV7 user ID is used. The audit trails should record who uses the IMSV7 and when, and also record what has been done to the system. The audit trail should be reviewed and analyzed in a timely manner by someone other than the programmer who uses the IMSV7. In addition, DIT should change IMSV7 password on a regular basis.

Management Response: In addition to the Security Policy Exemption memorandum dated March 25, 2008, DIT implemented an Oracle Script on September 1, 2009, that involves the daily execution and monitoring of an Oracle audit script that identifies the name, workstation ID, and login time of the person logging in as IMSV7. The script results are sent to the LPD Branch Chief, DIT Security Office, and the Enterprise Technology Operations Center for review. The LPD Branch Chief responds with appropriate documentation (i.e., Infra/CM#, or reason) that supports LPD staff IMSV7 activities as needed. Thus, the recommendation of generating and reviewing the audit trail for the IMSV7 user ID was implemented during the audit.

The long-term solution is in the replacement of the FIDO system, which should provide role-based administrative user IDs and the user IDs' passwords will be changed on a regular basis. The anticipated completion date is 2014.

IT Security Policy exemptions were not meant to deter DIT staff assigned to support systems without a waiver; thus, the Security Policy will be updated to clarify circumstances for appropriate support and accountability. The anticipated completion date is December 2010.

8. FIDO System Administrator Privileges

The FIDO system provided the system administrator the privilege to view in clear text the users' passwords in the user profiles list. Fairfax County Information Technology Security Policy 70-05.01 states: "An unencrypted password must not be written or stored in a location (physical or logical) in which any person other than the password owner has access." The FIDO system is a commercial-off-the-shelf product developed by Hansen Software Solution. This application has the built-in function to allow the system administrator to view users' passwords.

The User ID and password are used to identify and authenticate the user. Password identification and authentication is critical to every computer system. Personal passwords used to authenticate identity should be known only by the individual having identity.

Recommendation: We recommend that Department of Information Technology (DIT) coordinate with the vendor to remove the view access of user passwords function from the system administrator in the FIDO system.

Management Response: The FIDO system is a legacy commercial-off-the-shelf software package that has a unique 15 year old architecture and does not have a standard Oracle development tool embedded in the application. While we agree that the optimal situation is to implement encrypted passwords, this capability is not

available without a major software upgrade action. The FIDO application requires a new version release, which on initial delivery, DIT found several deficiencies through testing that must be corrected by the vendor before implementing and moving into production. The implementation process, once an acceptable version is provided, requires that all five FIDO agencies re-test all 113 application configurations (inspections, permits, and complaint types, etc.). Since the only persons that can view the passwords are the authorized system administration group in the DIT-LPD branch; and over the seven years under this constrained COTS system limitation, there have been no breaches. Under the current budget and resources limitations, we do not deem this a high-risk situation at this time. Also, we note that this application is being slated for replacement in several years to acquire a modern solution that meets industry and DIT software architecture and security standards.

Hansen's FIDO solution requires an upgrade; and because of the complexity of the FIDO configuration, this work requires complex testing to complete the upgrade without interrupting services. The new version of the FIDO application should remove the function that allows the system administrator to view users' passwords. The anticipated completion date is July 2011.

9. FIDO Application Password

The FIDO application did not require users to create strong passwords. It accepted a password with only one character during a test. The FIDO application's user ID was the employee's network ID, the initial password was the same as the FIDO application's user ID. The FIDO application did not require a user to change his/her initial password after the first sign-on. In addition, the passwords did not have expiration dates. The FIDO application is a commercial-off-the-shelf product developed by Hansen Software Solution. This application does not have the built-in functions to enforce strong passwords and periodic password changes.

DIT was working in the test environment to test whether the FIDO application could require a user to change his/her password every 90 days. DIT planned to test whether the FIDO application could require user to create a strong password.

Fairfax County Information Technology Security Policy 70-05.01 states that all passwords, including initial passwords, should be constructed and implemented according to the following complexity rules:

- It shall be routinely changed (at minimum, not longer than every 90 days).
- It shall adhere to a minimum length as established by DIT.
- It shall be a strong password as defined by DIT.
- It shall not be anything that can be easily tied back to the account owner such as: user name, Social Security number, nickname, relative's names, birth date, etc.
- It shall not be dictionary words or acronyms.
- Password history will be retained by systems to prevent the reuse of a password.

Password identification and authentication is critical to every computer system. Weak passwords cannot adequately protect permit applications from unauthorized modification, disclosure, loss, or impairment.

Recommendation: We recommend that the Department of Information Technology (DIT) implement the feature of requiring users to change passwords every 90 days. DIT should coordinate with the vendor to develop strong password features in the FIDO application that comply with the IT Security Policy.

In the meantime, DIT should require FIDO application users to change their passwords to no less than six alpha/numeric characters in compliance with the strong password requirements based on the County's Information Technology Security Policy 70-05.01.

Management Response: The FIDO COTS application cannot implement strong passwords. DIT does not deem this as a significant risk since this is a closed system; and thus, not deemed a high-risk based on actual experience and cost for a replacement system. We also note that no actual breaches of anyone not authorized to access the application have occurred. We note, however, that we have implemented a forced password change in lieu of the system deficiencies, which has caused additional system administration duties under already constrained support capacity.

On September 25, 2009, all FIDO user profiles were modified to force all FIDO users to change their passwords every 90 days. The user profile modifications became effective on September 28, 2009. The long-term solution is in the replacement of the FIDO system, which should provide a built-in function for requiring users to create strong passwords. The anticipated completion date is 2014.

10. Oracle Database Recovery

The county did not have the hardware to recover all Oracle databases. Only version 10G databases could be recovered at the Chantilly hot site. The Chantilly hot site did not have compatible servers to support version 9 and 8 Oracle databases. The current FIDO application Oracle database was version 9.2.6. The Oracle database must be upgraded to 10G in order to be recoverable.

Fairfax County Information Technology Security Policy 70-05.01 states that the Fairfax County information systems backup and recovery process for each system shall be documented and periodically reviewed. Backups shall be periodically tested to ensure that they are recoverable.

In the case of a disaster or incident affecting the DIT Data Center (where the servers are housed), the FIDO database cannot be recovered at the hot site, the impact on the county can be significant.

Recommendation: We recommend that DIT upgrade the FIDO Oracle database to 10G version and test the backups periodically to ensure that they are recoverable.

Management Response: DIT is not funded for full disaster recovery for all applications. DIT has a plan for migrating Oracle based applications to version 10, as certified by the COTS vendors for their system, and as time and resources permit. The FIDO application requires a new release, which on delivery DIT found several deficiencies through testing that must be corrected by the vendor before implementing and moving into production. The implementation process requires that all five FIDO agencies re-test all 113 application configurations (inspections, permits, and complaint types, etc.). That said, we also note in this response that we have not experienced any major hardware failures for the application; and like all agencies, a business COOP plan should be in place if a hardware failure should occur for a negotiated amount of time to allow for IT recovery. Absent an automatic fail-over, DIT is able to restore FIDO to an alternative platform under an extreme emergency.

The FIDO upgrade to Oracle 10.0 is planned as Hansen provides a working release, and agencies' testing can be planned and completed. The anticipated completion date is July 2011.